REMARKS

Applicant wishes to acknowledge with appreciation the allowance of claims 27 to 30. Claims 25 and 26 are objected to as depending from a rejected claim but are otherwise considered allowable if written independently and include all the limitations of the claims from which they depend. Independent claims 23 and 31 are still rejected, and claim 24, dependent from rejected claim 23 is also rejected. If applicant can persuade the Examiner that claim 23 is allowable, then, claim 24 would also be allowable.

The application has been carefully reviewed in light of the Office Rejection, and with all due respect, it appears that the rejection of claims 23, 24 and 31 is predicated upon a misconception of the purpose of "the K combinatorial circuits that compute F, where K is a security parameter", how they function and are being used in the claimed combinations.

If applicant is reading the Office Action correctly, particularly on page 4, concerning the combination of the Ausubel and Micali references, it appears that the Examiner is of the impression that the K security combinatorial parameter is a common key and that c.sub.i is an encrypted bid using the common key, somewhat in the manner of the Micali reference. If applicant's understanding of the Examiner's impression is accurate, then this impression is a misconstruction of the claims.

According to claims 23 and 31, the purpose and function of "the K combinatorial circuits that compute F, where K is a security parameter" is to insure the trust-worthiness of the auction controlling center or entity that is controlling the auction. These K combinatorial circuits are not a common key and have absolutely nothing whatsoever to do with encryption.

Quite apart from Micali, the encryption in claims 23 and 31 takes place exclusively by and under the control of each individual bidder, so the encryptions by the bidders can all be different. Each bidder, initially submits his commitment to bid to the auction controlling entity with the actual

bidding information under encryption **[limitation d, claims 23 and 31]**. However, the controlling entity **cannot** decrypt the commitment because it does not have the necessary decryption data. Next, the auction controlling entity starts to prove its trust-worthiness by making a commitment to use the K combinatorial circuits **[limitation e, claims 23 and 31]**. Then the auction controlling entity continues to prove its trust-worthiness by providing part of the K combinatorial circuits to each bidder **[limitation f, claims 23 and 31]**. When the bidders are satisfied that the auction controlling center has prima facie trust-worthiness, the bidders then each give the auction controlling center his decryption data so the auction controlling center can now decrypt each bidder's bid **[limitation g, claims 23 and 31]**. Then the auction controlling center calculates function F using the portion of the K combinatorial circuits it withheld from the bidders **[limitation h, claims 23 and 31]**, and publishes the result to the bidders, together with a proof that it calculated the result correctly. Each bidder can verify the correctness of the result by using the published F, his bid and the part of the K combinatorial circuits he has access to **[limitation I, claims 23 and 31]**, thereby verifying the trust-worthiness of the auction controlling entity.

As will be evident form the above, the purported combination of references does not anticipate or render obvious claims 23 and 31. It is respectfully solicited that claims 23, 24 and 31 are patentably distinguishable over the references cited of record and applied.

In light of the foregoing remarks, this application should be in condition for allowance, and early passage of this case to issue is respectfully requested. If there are any questions regarding this amendment or the application in general, a telephone call to the undersigned would be appreciated since this should expedite the prosecution of the application for all concerned.

It is respectfully requested that, if necessary to effect a timely response, this paper be considered as a Petition for an Extension of Time, time sufficient, to effect a timely response, and shortages in this or other fees, be charged, or any overpayment in fees be credited, to the Deposit Account of the undersigned, Account No. 500601 (Docket no. 704-X99-043)

Respectfully submitted,

Martin Fleit

Martin Fleit, Reg. #16,900

Martin Fleit
FLEIT KAIN GIBBONS GUTMAN & BONGINI
21355 East Dixie Highway, Suite 115
Miami, Florida 33180
Tel: 305-830-2600; Fax: 305-830-2605
e-mail: MFleit@Focusonip.com